

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A)

平4-117826

⑬ Int. Cl.<sup>9</sup>

識別記号

庁内整理番号

⑭ 公開 平成4年(1992)4月17日

H 04 L 9/28  
G 09 C 1/00

7922-5L  
7117-5K

H 04 L 9/02

A

審査請求 未請求 請求項の数 1 (全7頁)

⑮ 発明の名称 認証機能付き鍵配送方式

⑯ 特 願 平2-237498

⑰ 出 願 平2(1990)9月7日

⑱ 発 明 者	松 崎 な つ め	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑱ 発 明 者	原 田 俊 治	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑱ 発 明 者	館 林 誠	大阪府門真市大字門真1006番地	松下電器産業株式会社内
⑲ 出 願 人	松下電器産業株式会社	大阪府門真市大字門真1006番地	
⑳ 代 理 人	弁理士 小 鍛 治 明	外2名	

明 細 書

1. 発明の名称

認証機能付き鍵配送方式

2. 特許請求の範囲

重複しない固有の識別情報を持った第1、第2の端末と、端末間を結ぶ通信路と、各端末が生成した公開情報に署名を施して証明書を発行するセンターとからなるシステムにおいて、証明書の発行時は、前記第1の端末は秘密情報x1を生成し、システムで公開の数pとpを法とする剰余環の原始元gを用いてx1をべきとし前記pを法とするgのべき乗剰余値y1を算出し、このy1を第1の公開情報としてセンターに通知し、前記第2の端末は秘密情報x2を生成し、x2をべきとし前記pを法とするgのべき乗剰余値y2を算出し、このy2を第2の公開情報としてセンターに通知し、センターは前記第1、2の公開情報に端末の識別情報を含めて、署名を施して証明書を生成し、各端末それぞれに配付し、鍵配送時、前記第1の端末は、前記通信路に接続し、前記センターから配付された第1の端末の証

明書を格納して、通信路を通じて第2の端末に送信する第1の証明書格納手段と、乱数r1を生成する第1の乱数発生手段と、前記第1の乱数発生手段と前記通信路に接続し、前記r1をべきとし前記pを法とするgのべき乗剰余値C1を算出して、前記通信路を通じて第2の端末にデータC1を送信する第1の送信データ生成手段から構成され、前記第2の端末は、前記通信路に接続し、前記センターから送信された第2の端末の証明書を格納して、通信路を通じて第1の端末に送信する第2の証明書格納手段と、前記第1の端末から送信された第1の端末の証明書から第1の端末の第1の公開情報y1を求める第1の公開情報算出手段と、乱数r2を生成する第2の乱数発生手段と、前記第2の乱数発生手段と前記通信路に接続し、前記r2をべきとし前記pを法とするgのべき乗剰余値C2を算出して、前記通信路を通じて第1の端末にデータC2を送信する第2の送信データ生成手段と、前記第2の端末の秘密情報x2を格納する第1の秘密情報格納手段と、前記第1の秘密情報格納手段と前記第

2の乱数発生手段と前記通信路に接続し、前記乱数 $r_2$ と第2の端末の秘密情報 $x_2$ の和をべきとし、前記 $p$ を法とする前記送信データ $C_1$ のべき乗剰余値 $R_2$ を算出し、前記通信路を通じて第1の端末にデータ $R_2$ を送信する第3の送信データ生成手段から構成され、前記第1の端末は、前記第2の端末から送信された第2の端末の証明書から第2の端末の公開情報 $y_2$ を求める第2の公開情報算出手段と、前記第2の公開情報算出手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数 $r_1$ をべきとし前記 $p$ を法とする前記 $C_2$ と $y_2$ の積のべき乗剰余値を求め、これと前記第2の端末から送信された第3の送信データ $R_2$ を比較してこれらが同じであることによって第2の端末を認証する第1の認証手段と、前記第1の端末の秘密情報 $x_1$ を格納する第2の秘密情報格納手段と、前記第2の秘密情報格納手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数 $r_1$ と第1の端末の秘密情報 $x_1$ の和をべきとし、前記 $p$ を法とする前記第2の送信データ $C_2$ のべき乗剰余値 $R_1$ を算出し、前記通信路

-3-

### 3. 発明の詳細な説明

#### 産業上の利用分野

本発明は、互いにチャレンジとレスポンスをやり取りすることによって相手を認証し、その結果秘密の共有鍵を得る認証機能付き鍵配送方式に関する。なお、相手からのレスポンスの正当性確認に用いる相手端末の公開情報は、信頼のおけるセンターがあらかじめ生成した証明書によって保証されている。

#### 従来の技術

暗号系に秘密鍵暗号方式を用いる場合、各通信対で対ごとに異なった鍵を秘密に共有する必要がある。従来の集中鍵配送方式では、鍵共有のたびに、ネットワーク上にある鍵配送センターが各共有鍵を生成し、端末に秘密に配送する必要があるため、鍵配送センターに鍵負担が集中し、端末数の多い大規模ネットワークには適していない。一方、鍵の配送と同時に、鍵を共有する相手をきちんと認証することも要望されている。したがって、ここでは認証機能を組み込んだ分散型の鍵配送方

-5-

を通じて第2の端末にデータ $R_1$ を送信する第4の送信データ生成手段と、前記第1の乱数発生手段と前記通信路に接続し、乱数 $r_1$ をべきとし前記 $p$ を法とする前記第2の端末から送信された第2の送信データ $C_2$ のべき乗剰余値を、前記第2の端末との共有鍵とする第1の共有鍵生成手段から構成され、前記第2の端末は、前記第1の公開情報算出手段と前記第2の乱数発生手段と前記通信路に接続し、前記乱数 $r_2$ をべきとし前記 $p$ を法とする前記 $C_1$ と $y_1$ の積のべき乗剰余値を求め、これと前記第1の端末から送信された第4の送信データ $R_1$ を比較してこれらが同じであることによって第1の端末を認証する第2の認証手段と、前記第2の乱数発生手段と前記通信路に接続し、乱数 $r_2$ をべきとし前記 $p$ を法とする前記第1の端末から送信された第1の送信データ $C_1$ のべき乗剰余値を前記第1の端末との共有鍵とする第2の共有鍵生成手段から構成される認証機能付き鍵配送方式。

-4-

式について説明する。分散型の鍵配送方法として、1976年にディフィとヘルマン(Diffe, Hellman)によって提案されたディエイチ(DH)鍵配送方式がある。詳細については、アイイーイーイー・トランザクションズ・オン・インフォメーション・セオリー(IEEE Trans. Inf. Theory IT-22, 6, pp644~654(Nov. 1976))を参照すること。DH鍵配送方式は有限体 $GF(p)$ 上での離散対数問題が難しいことに安全性の根拠をおいている。ここではこれに認証機能を組み込んだ方法について説明する。認証を可能とするため、信頼のおけるセンター発行の証明書を用いる。

#### DH鍵配送方式(第1の従来例)

以下、この第1の従来例の手順を、センターによる証明書の発行のフェーズと、端末1と端末2の間の鍵配送のフェーズに分けて説明する。

#### <証明書の発行フェーズ>

(1) システムの構築時、素数 $p$ と $GF(p)$ の原始元 $g$ を決定し各端末に公開する。ここで安全性を確保するため、 $p$ は例えば512ビット程度の大きな素

-6-

数に決定する。

(2) 端末1は秘密情報 $x_1$ を生成して、 $y_1 = g^{x_1} \bmod p$ を計算する。

なお、ここで ' $X \bmod p$ ' は値 $X$ を $p$ で除した時の剰余を示す。

(3) 端末1は $y_1$ と名前、住所など自分を特定できる情報(識別情報、又はID情報と称する)ID1を信頼のおけるセンターに送信し、証明書を請求する。

(4) センターは端末1の正当性を調べ、センターだけが知っている秘密変換 $f$ を用いて、証明書 $Cert1$ を生成し、例えば磁気カード等に格納して端末1に配付する。

$Cert1 = f(y_1 \parallel ID1)$

ここで、 $\parallel$ は連結を示している。なお、秘密変換 $f$ の逆変換 $h$ はシステムにおいて公開であるとする。従って、 $Cert1$ を得た任意の端末は $h(Cert1)$ を計算することで、センターによって保証された端末1の公開情報 $y_1$ を得ることができる。端末2についても同様に証明書 $Cert2$ を発行する。

-7-

鍵を変更する方法が提案されている。証明書の発行フェーズは第1の従来例と同じである。第2図に鍵配送フェーズの手順を示している。端末1、2間の動作を以下に示す。

(1) 端末1は次のようにして配送情報 $Z12$ を生成し、これと自分の証明書 $Cert1$ を端末2に送付する。

(a) 乱数 $r_1$ を発生する。

(b)  $Z12 = y_1^{r_1} \bmod p \quad \dots (1)$

(2) 端末2は次のようにして配送情報 $Z21$ を生成し、これと自分の証明書 $Cert2$ を端末1に送付する。

(a) 乱数 $r_2$ を発生する。

(b)  $Z21 = y_2^{r_2} \bmod p \quad \dots (2)$

また、端末1から送付されてきた情報を用いて、以下のとおり端末1との共有鍵 $K21$ を生成する。

(a)  $Cert1$ より、 $h(Cert1) = y_1 \parallel ID1$ を計算し、センターの認めた端末1の公開情報 $y_1$ を得る。

(b) 端末1からの配送情報 $Z12$ より次のように共有鍵を算出する。

< 鍵配送フェーズ >

(1) 端末1は自身の証明書 $Cert1$ を端末2に、端末2は自身の証明書 $Cert2$ を端末1にそれぞれ配送する。

(2) 端末1は $h(Cert2) = y_2 \parallel ID2$ を計算し、自分の秘密情報 $x_1$ を用いて、

$K12 = y_2^{x_1} \bmod p = g^{x_1 x_2} \bmod p$

を求める。

(3) 一方、端末2は $h(Cert1) = y_1 \parallel ID1$ を計算し、自分の秘密情報 $x_2$ を用いて、

$K21 = y_1^{x_2} \bmod p = g^{x_1 x_2} \bmod p$

を求める。なお、 $K12 = K21$ は端末1と2の間の共有鍵である。

ところで、暗号通信で用いられる暗号鍵は、安全上時々変更することが望ましい。上記で述べたDH鍵配送方式では共有鍵を変更するのにもう1度センターに依頼して証明書を発行してもらう必要があり、非常に手間である。

第2の従来例

特開昭61-30829では、証明書は変更せずに共有

-8-

$K21 = (Z12 \times y_1^{r_2})^{x_2} \bmod p \quad \dots (3)$

(3) 端末1は、端末2から送付されてきた情報を用いて、以下のとおり端末2との共有鍵共有鍵 $K12$ を生成する。

(a)  $Cert2$ より、 $h(Cert2) = y_2 \parallel ID2$ を計算し、センターの認めた端末2の公開情報 $y_2$ を得る。

(b) 端末2からの配送情報 $Z21$ より次のように共有鍵を算出する。

$K12 = (Z21 \times y_2^{r_1})^{x_1} \bmod p \quad \dots (4)$

なお、端末1における共有鍵 $K12$ と端末2における共有鍵生成手段 $K21$ は(1)~(4)式より同じ値になる。

$K12 = (Z21 \times y_2^{r_1})^{x_1} \bmod p = (y_2^{r_2 r_1})^{x_1} \bmod p = x_1 r_1 r_2 \bmod p$

$K21 = (Z12 \times y_1^{r_2})^{x_2} \bmod p = (y_1^{r_1 r_2})^{x_2} \bmod p = x_2 r_1 r_2 \bmod p$

発明が解決しようとする課題

第1の従来例では、特定の2者間の鍵が毎回同じであるという欠点がある。第1の従来例で毎回の鍵を変更するためには、センターにおいて端末

-9-

-10-

の証明書を作り替えてもらわなくてはならず、かなり手間がかかる。また、第2の従来例では証明書を変更せずに毎回の鍵を変更することができる。但し、この方式における認証機能は間接的な認証であり、自分の認識している相手とのみ同じ鍵を共有できることが保証されているというものであった。従って、きちんと相手からのデータにより相手を認証するものではない。さらに共有鍵を得るには、配送データの生成に1回、共有鍵の生成に2回の計3回のべき乗剰余演算が必要である。本発明の認証機能付き鍵配送方式は、上述の問題点に鑑みて試みられたもので、証明書を変更せずに毎回の鍵を変更する鍵配送方式であって、さらに、相手にデータ（チャレンジ）を与え、その応答（レスポンス）によってきちんと相手を検証する認証機能を付加した鍵配送方式を提供することを目的とする。なお、この際に従来の間接的認証を付加した方法に比べて計算量の増加を最小限とする。

-11-

の証明書格納手段と、乱数 $r_1$ を生成する第1の乱数発生手段と、前記第1の乱数発生手段と前記通信路に接続し、前記 $r_1$ をべきとし前記 $p$ を法とする $g$ のべき乗剰余値 $C_1$ を算出して、前記通信路を通じて第2の端末にデータ $C_1$ を送信する第1の送信データ生成手段から構成され、前記第2の端末は、前記通信路に接続し、前記センターから送信された第2の端末の証明書を格納して、通信路を通じて第1の端末に送信する第2の証明書格納手段と、前記第1の端末から送信された第1の端末の証明書から第1の端末の第1の公開情報 $y_1$ を求める第1の公開情報算出手段と、乱数 $r_2$ を生成する第2の乱数発生手段と、前記第2の乱数発生手段と前記通信路に接続し、前記 $r_2$ をべきとし前記 $p$ を法とする $g$ のべき乗剰余値 $C_2$ を算出して、前記通信路を通じて第1の端末にデータ $C_2$ を送信する第2の送信データ生成手段と、前記第2の端末の秘密情報 $x_2$ を格納する第1の秘密情報格納手段と前記第1の秘密情報格納手段と前記第2の乱数発生手段と前記通信路に接続し、前記乱数 $r_2$ と第2の端末の

-13-

#### 課題を解決するための手段

前記目的を達成するために、本発明における認証機能付き鍵配送方式は、重複しない固有の識別情報を持った第1、第2の端末と、端末間を結ぶ通信路と、各端末が生成した公開情報に署名を施して証明書を発行する信頼のおけるセンターからなるシステムにおいて、証明書の発行時は、前記第1の端末は秘密情報 $x_1$ を生成し、システムで公開の数 $p$ と $p$ を法とする剰余環の原始元 $g$ を用いて $x_1$ をべきとし前記 $p$ を法とする $g$ のべき乗剰余値 $y_1$ を算出し、この $y_1$ を第1の公開情報としてセンターに通知し、前記第2の端末は秘密情報 $x_2$ を生成し $x_2$ をべきとし前記 $p$ を法とする $g$ のべき乗剰余値 $y_2$ を算出し、この $y_2$ を第2の公開情報としてセンターに通知し、センターは前記第1、2の公開情報に端末の識別情報を含めて、署名を施して証明書を生成し、各端末それぞれに配付し、鍵配送時、前記第1の端末は、前記通信路に接続し、前記センターから配付された第1の端末の証明書を格納して、通信路を通じて第2の端末に送信する第1

-12-

秘密情報 $x_2$ の和をべきとし、前記 $p$ を法とする前記送信データ $C_1$ のべき乗剰余値 $R_2$ を算出し、前記通信路を通じて第1の端末にデータ $R_2$ を送信する第3の送信データ生成手段から構成され、前記第1の端末は、前記第2の端末から送信された第2の端末の証明書から第2の端末の公開情報 $y_2$ を求める第2の公開情報算出手段と、前記第2の公開情報算出手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数 $r_1$ をべきとし前記 $p$ を法とする前記 $C_2$ と $y_2$ の積のべき乗剰余値を求め、これと前記第2の端末から送信された第3の送信データ $R_2$ を比較してこれらが同じであることによって第2の端末を認証する第1の認証手段と、前記第1の端末の秘密情報 $x_1$ を格納する第2の秘密情報格納手段と、前記第2の秘密情報格納手段と前記第1の乱数発生手段と前記通信路に接続し、前記乱数 $r_1$ と第1の端末の秘密情報 $x_1$ の和をべきとし、前記 $p$ を法とする前記第2の送信データ $C_2$ のべき乗剰余値 $R_1$ を算出し、前記通信路を通じて第2の端末にデータ $R_1$ を送信する第4の送信データ生成手

-14-

段と、前記第1の乱数発生手段と前記通信路に接続し、乱数 $r_1$ をべきとし前記 $p$ を法とする前記第2の端末から送信された第2の送信データ $C_2$ のべき乗剰余値を、前記第2の端末との共有鍵とする第1の共有鍵生成手段から構成され、前記第2の端末は、前記第1の公開情報算出手段と前記第2の乱数発生手段と前記通信路に接続し、前記乱数 $r_2$ をべきとし前記 $p$ を法とする前記 $C_1$ と $y_1$ の積のべき乗剰余値を求め、これと前記第1の端末から送信された第4の送信データ $R_1$ を比較してこれらが同じであることによって第1の端末を認証する第2の認証手段と、前記第2の乱数発生手段と前記通信路に接続し、乱数 $r_2$ をべきとし前記 $p$ を法とする前記第1の端末から送信された第1の送信データ $C_1$ のべき乗剰余値を前記第1の端末との共有鍵とする第2の共有鍵生成手段から構成される。

作用

第2の端末は第1の端末の出力するチャレンジデータ $C_1$ に対するレスポンス $R_2$ を、自分の秘密情報 $x_2$ と自分の生成した乱数 $r_2$ を用いて生成する。

-15-

(2) 端末2は次のようにして配送情報 $C_2$ を生成する。

(a) 乱数 $r_2$ を発生する。

(b)  $C_2 = g^{r_2} \text{ mod } p$

また、前記 $C_1$ に対するレスポンスとして以下の $R_2$ を生成する。そして自分の証明書 $CERT_2$ とともに前記 $C_2$ 、 $R_2$ を第1の端末に送信する。

$R_2 = C_1^{r_2 \cdot x_2} \text{ mod } p$

(3) 端末1は端末2から送信された証明書 $Cert_2$ から

$h(Cert_2) = y_2 \parallel I D_2$

を計算し、センターが認めた端末2の公開鍵 $y_2$ を得る。次に、この公開鍵 $y_2$ を用いて、

$R_2 = (C_2 \times y_2)^{r_1} \text{ mod } p$

が成り立つことを確かめる。もし成り立てば、通信相手が端末2であることを認証し、次の計算で端末2との共有鍵を求める。異なっていれば、この鍵配送プロトコルを取りやめる。

$K_{12} = C_2^{r_1} \text{ mod } p$

また、前記第2の端末からチャレンジ $C_2$ に対す

従って、このレスポンスは正規の第2の端末しか生成することができない。第1の端末はこのレスポンスを、第2の端末の証明書から得た正規の公開情報 $y_2$ によって認証する。また、レスポンスに自分の生成した秘密の乱数 $r_2$ を含めているため、第1の端末および第3者はレスポンスから第2の端末の秘密情報 $x_2$ を得ることはできない。同様に、端末2はチャレンジデータ $C_2$ に対するレスポンス $R_1$ により端末1を認証する。そして互いに相手を認証した後、相手からのチャレンジデータを用いて共有鍵を求める。

実施例

第1図は、本発明の認証機能付き鍵配送方式の鍵配送フェーズにおけるプロトコルを示す。証明書発行フェーズは従来例と同じである。

(1) 端末1は次のようにして配送情報 $C_1$ を生成し、これと自分の証明書 $Cert_1$ を端末2に送付する。

(a) 乱数 $r_1$ を発生する。

(b)  $C_1 = g^{r_1} \text{ mod } p$

-16-

るレスポンスとして以下の $R_1$ を生成する。そして第1の端末に送信する。

$R_1 = C_2^{r_1 \cdot x_1} \text{ mod } p$

(4) 端末2は端末1から送信された証明書 $Cert_1$ から

$h(Cert_1) = y_1 \parallel I D_1$

を計算し、センターが認めた端末1の公開鍵 $y_1$ を得る。次に、この公開鍵 $y_1$ を用いて、

$R_1 = (C_1 \times y_1)^{r_2} \text{ mod } p$

が成り立つことを確かめる。もし成り立てば、通信相手が端末1であることを認証し、次の計算で端末1との共有鍵を求める。異なっていれば、この鍵配送プロトコルを取りやめる。

$K_{21} = C_1^{r_2} \text{ mod } p$

なお、 $K_{12} = K_{21} = g^{r_1 \cdot r_2 \cdot x_1 \cdot x_2} \text{ mod } p$ である。

この実施例において、相手からチャレンジに対するレスポンスを生成するためには、正規の秘密情報が必要である。そして、このレスポンスをセンターの認めた公開情報を用いて確認する。このため、この方法は直接的な相手認証を含んだ鍵配

-17-

-18-

送方式であるといえる。なお、鍵の共有は相手からうけたチャレンジを用いDH鍵配送方式と同様に行なう。また、鍵共有までの計算量については以下の通り評価する。なお、計算量の評価はべき乗剰余演算の回数を行なう。これは、安全性を確保する（公開情報から端末の秘密情報を得ることを困難にする）ために各計算の法 $p$ の数を大きく（例えば512ビット）取ると、べき乗剰余演算が全体の計算時間のネックとなるためである。双方の端末ともに

- ・チャレンジの生成に1回
- ・レスポンスの生成に1回
- ・相手のレスポンスの正当性確認に1回
- ・共有鍵の生成に1回

の計4回のべき乗剰余演算が必要である。従って、従来の間接的な認証機能が付加された鍵配送方式に比べてわずか1回のべき乗剰余演算が増加しているだけである。なお、この実施例では、チャレンジとレスポンスを用いた認証を鍵配送と合わせて構成したが、認証方式単独として取り扱

てもよいことは言うまでもない。

#### 発明の効果

以上の説明から明らかなように本発明は、証明書を変更せずに毎回の共有鍵を変更することができる。また、相手を自身が発したチャレンジに対する応答を、センターの認めた相手の公開鍵を用いて直接的に確認する。チャレンジとレスポンスによる相手認証では、レスポンスに秘密の乱数を含めることによって端末の秘密情報を保護している。また、これにかかる計算量はべき乗剰余演算4回であり、間接的な認証しかできなかった従来の鍵配送方式と比べても最小限の計算量の増加となっている。

#### 4. 図面の簡単な説明

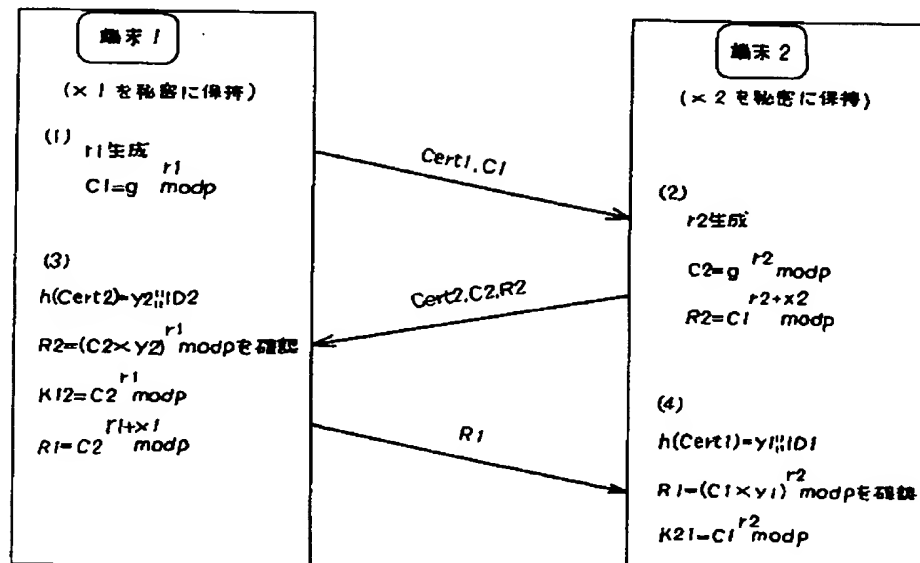
第1図は本発明の認証機能付き鍵配送方式における一実施例の鍵配送フェーズプロトコル図。第2図は従来における鍵配送フェーズプロトコル図である。

代理人の氏名 弁理士 小銀治 明 ほか2名

-19-

-20-

第 1 図



第 2 図

